

Case Summaries: Fourth Circuit Court of Appeals (March 3, 5, 10, 27, & 30, 2026)

Material dispute of fact precluded summary judgment; deputy not entitled to qualified immunity on excessive force claim

[Barricks v. Wright](#), 168 F.4th 210 (March 3, 2026). Around 9:30 p.m. in Covington, Virginia, a deputy on patrol noticed the plaintiff skateboarding on the street. The deputy was on the phone with his girlfriend at the time and remarked to her that, “this motherfu-ker’s skating down the Godd-mn road.” He turned his patrol car around and encountered the plaintiff in front of a local convenience store. While interacting with the plaintiff, the deputy suspected that the plaintiff was impaired by drugs. The plaintiff denied that he was impaired and told the deputy that the store clerk inside could verify that he had been gambling inside the store all day. When the deputy seemingly moved to grab the plaintiff, he pulled away, shouting at the deputy, “Man, that bullshi-t dude. Go ahead and shoot me!” The plaintiff then ran into the convenience store. The plaintiff ran to a backroom of the store where the deputy confronted him. The plaintiff fell to his knees and raised his hands up as the deputy yelled at the plaintiff to get on the ground. The plaintiff responded that he was already on the ground and laced his hands around the back of his head. The deputy’s bodycam captured the events up to this point but did not clearly depict what happened next. According to the plaintiff, his next memory was waking up in the hospital. According to the deputy, the plaintiff resisted being arrested, so the deputy used so-called “distraction strikes” to subdue him. The video showed the deputy pushing the plaintiff’s face to the floor and pulling the plaintiff’s wrist to handcuff him, and it appeared that the plaintiff resisted the arrest. The parties disputed whether the deputy used his knuckles to strike the plaintiff instead of an open palm or hand. After arresting him, the deputy found a small bag of what he believed to be methamphetamine. The plaintiff suffered “a facial laceration, facial bruising and swelling, and bruising on the knees,” as well as a “right frontal 6 mm intracerebral hemorrhage, closed fracture of the right orbital rim, blood in the maxillary sinus, and several fractures to two different parts of his jaw bone.” *Barricks* Slip op. at 2.

The plaintiff sued the deputy in the Western District of Virginia for excessive force. The district court denied the deputy’s motion for summary judgment, finding genuine disputes of material fact on the question of excessive force. It also determined that qualified immunity would not be appropriate because, if the jury found the disputed facts in the plaintiff’s favor, the use of force would have clearly been excessive under established law. The deputy appealed that ruling, renewing his argument that he was entitled to qualified immunity. A unanimous panel of the Fourth Circuit affirmed. Under *Graham v. Conner*, 490 U.S. 386, 396 (1989), whether an officer’s use of force was excessive is determined by examining the “circumstances of the case, including the severity of the crime at issue, whether the suspect posed an immediate threat to the safety of the officers or others, and whether he was actively resisting arrest or attempting to evade arrest by flight.” (cleaned up). Here, the plaintiff was being arrested for skateboarding on a public road and potentially public intoxication, both of which are nonviolent misdemeanors. The plaintiff had seemingly surrendered at the time, having raised his hands above his head and dropped to his knees in place. The plaintiff did not appear to pose a threat to the

officer or others. “In short, the facts taken in the light most favorable to Barricks would show that Deputy Wright applied gratuitous and injurious force after Barricks had surrendered and was no longer resisting.” *Barricks* Slip op. at 10. Circuit precedent clearly established that such force used against a person who has stopped resisting is excessive, and a jury could reasonably find the disputed facts in the plaintiff’s favor. Those factual disputes required resolution by a jury. The district court’s ruling denying the deputy qualified immunity at this stage was therefore affirmed.

Attorney’s advice that defendant would be deportable but may have other options to contest removal was correct and did not constitute deficient performance

[U.S. v. Murillo](#) (“*Murillo II*”), 169 F.4th 273 (March 5, 2026). The defendant was indicted in 2016 in the Eastern District of Virginia for possession of cocaine with intent to distribute and conspiracy to distribute a kilogram of cocaine. His defense lawyer negotiated a plea bargain to the conspiracy offense only, thus avoiding a mandatory minimum five-year sentence. The lawyer also negotiated several immigration-related terms out of the plea agreement, such as an agreement not to contest removal and to waive the right to seek asylum. The final plea agreement, however, still included a statement acknowledging that the defendant’s desire to plead guilty regardless of any potential immigration impacts, including the potential for mandatory removal from the country. During the plea colloquy, the district court and defense counsel advised the defendant that deportation was possible and something that “may” happen following his guilty plea. The defendant was sentenced to 24 months.

Soon after beginning his sentence, the defendant learned that he was likely to face mandatory deportation at the end of his sentence. He filed for habeas relief, arguing that his lawyer was ineffective for failing to advise him of that consequence. The district court denied the claim without holding a hearing, finding that the defendant could not demonstrate prejudice and pointing to the immigration-related term in his plea agreement. He appealed, and the Fourth Circuit reversed. In *Murillo I*, 927 F.3d 808 (4th Cir. 2019), the court found that the defendant had made a sufficient showing of prejudice for an ineffective assistance of counsel claim. It determined that the district court gave too much weight to the immigration condition in the plea agreement and should instead have asked whether the defendant would have rejected the plea if he had known that deportation was mandatory. The Fourth Circuit remanded the case for the district court to consider whether the defendant could show deficient performance by his plea counsel.

On remand, the district court held an evidentiary hearing at which the defendant’s trial counsel and another attorney from that lawyer’s firm who practices immigration law (and who advised the defendant about immigration consequences before the plea) both testified. The defendant, who had already been deported at that point, argued through counsel that his plea attorney’s failure to advise him of the mandatory immigration consequences constituted deficient performance. The district court disagreed. The defendant’s plea attorney advised him that he would become “deportable” and “removable,” while also explaining that deportation or removal was not an absolute certainty. This, to the district court, met the constitutional minimum to for advising the defendant about the immigration consequences of his plea.

The defendant again appealed, and a divided panel of the Fourth Circuit affirmed. “[Defendant’s plea counsel] did not impart any incorrect advice or fail to notify [the defendant] that there would be deportation consequences to his guilty plea.” *Murillo* Slip op. at 22. Plea counsel informed the defendant that he was pleading to an aggravated felony and that the plea would render him deportable. Plea

counsel's advice that there may be other potential, if narrow, avenues of immigration relief was correct. Thus, "[the defendant] failed to demonstrate that [plea counsel] was constitutionally required to advise him that he was ineligible for any relief from deportation and thus would, in fact, be found deportable." The district court was therefore correct in concluding that the defendant could not show deficient performance and properly denied his petition for habeas relief.

Judge Thacker dissented. She would have found deficient performance and granted the defendant's requested relief.

Defendant retained a reasonable expectation of privacy in Google Drive files despite Google's privacy policy and despite the contraband nature of the images within the files; law enforcement exceeded Google's private search of the files; evidence was sufficiently attenuated from the illegal search, rendering suppression inappropriate

[U.S. v. Lowers](#), 170 F.4th 134 (March 10, 2026). Google takes voluntary steps to identify and remove child sexual abuse material ("CSAM") from its services. Google often finds such material through a process known as "hash-matching." Digital files on Google servers are assigned specific hash values based on the content of the file. The assigned hash value is then checked against a database of the hash values of known CSAM images. A match means that the two images are likely the same (although the exact degree of accuracy of a hash-match is unclear). When the algorithm detects possible CSAM, a Google employee who has been trained to identify CSAM examines the suspicious file. If the reviewer confirms that the file contains probable CSAM, the file is identified as such, the file's hash value is placed into the database of suspected CSAM images, and a report is made about the file to the National Center for Missing and Exploited Children ("NCMEC"). This process allows Google to identify other files containing the same or similar CSAM on Google servers as new files are uploaded to the system. When the hash-value of a new file matches a known hash-value in Google's database, Google investigators sometimes open the suspicious file to verify the likely presence of CSAM before sending the report to NCMEC, but sometimes this step is skipped and the report is made directly to NCMEC without additional human review of the image (since a hash-match presumably means that a reviewer already examined the matching image before it was placed into Google's database of suspected CSAM at some point in the past). When making the report to NCMEC, Google indicates whether a reviewer has opened and viewed the suspicious image. Google's privacy policy cautions users that Google proactively tries to identify CSAM on its servers and will report suspected CSAM to law enforcement.

In 2019, someone associated with a particular email address uploaded 156 files to Google Drive, a digital file storage platform. Google quickly identified each of the files as probable CSAM. A human reviewer opened 31 of the 156 files and determined that each file contained likely CSAM. A report was made to NCMEC noting that around 20% of the files had been opened and reviewed, but 80% of the files had not. A worker with NCMEC reviewed the same 31 files and did not open the unviewed files. The employee determined that the IP address connected with the upload came from Bedford County, Virginia, and forwarded the report to local law enforcement. Local law enforcement took no action for six months. When an investigator began working on the report, they subpoenaed the internet service provider for account information connected to the IP address. From that information, law enforcement determined that the residence connected to the IP address was in Chesapeake, Virginia, and not Bedford County. Bedford County law enforcement therefore passed the report along to the Chesapeake police and closed their file.

After receiving the file, a detective with Chesapeake police opened at least three files containing images that neither Google nor NCMEC had previously opened. She confirmed that each file contained CSAM. The detective did not obtain a search warrant before doing so. She then sought and received a search warrant for the email account that had uploaded the files. That information showed that the account had been created expressly for the purpose of uploading the files—the account went inactive in less than 30 minutes after it was created and had not been used again since. The detective conducted surveillance on the home connected with the account for four months but did not obtain any new information. Eventually, she sought a search warrant for the home, explaining in her affidavit that she had seen three images of CSAM that originated from an email account connected to the home. A married couple with two young children lived in the house. Law enforcement searched ten digital devices but found no CSAM. During an interview with the police, the husband reported that their 21-year-old son had recently moved from their home to Raleigh, North Carolina. Chesapeake police therefore closed their file and reported what they knew about the case to Raleigh police.

A Raleigh detective and an agent from Homeland Security contacted the son, who agreed to speak with the men. He denied knowing anything about the Google account but consented to a search of his cell phone and computer. Police found four images of CSAM that had been deleted on the phone. Police again interviewed the young man. This time, he confessed that he downloaded CSAM from his parent's home onto a flash drive and transported the flash drive to Raleigh. He informed the officers where they could locate the flash drive in his apartment. While this second interview was being conducted, other law enforcement agents were already searching the suspect's apartment pursuant to a search warrant. Those officers found the flash drive with hundreds of CSAM images and over a dozen videos of CSAM, along with a hard drive with additional video and over 750 CSAM images.

The defendant was indicted in the Eastern District of North Carolina for possessing and transporting CSAM. All the charges related to images found in the defendant's apartment; he was not charged with the images uploaded to the Google Drive account. The defendant moved to suppress. He argued that the Chesapeake detective's act of opening the three images that had not previously been viewed by Google or NCMEC violated his reasonable expectation of privacy and violated the Fourth Amendment. The district court denied the motion, finding that the detective's actions did not amount to a search. Given Google's privacy policy and the warning to users that Google takes steps to identify CSAM on its platforms, the district court concluded that the defendant did not have an objectively reasonable expectation of privacy in his Google cloud account.

In the alternative, even assuming the defendant had a reasonable expectation of privacy in his cloud account, he did not have a reasonable expectation of privacy in the files because they were contraband and "nobody has an expectation of privacy in contraband." *Lowers Slip op.* at 11. The district court also held in the alternative that Google's private search of the files defeated any expectation of privacy in the file that the defendant may have had. Assuming arguendo that the search was unconstitutional, the district court further found that the detective reasonably relied on the federal statute that requires internet service providers to report CSAM to law enforcement which (according to the district court) allowed a warrantless search of the files. The good-faith exception therefore would have precluded suppression. Finally, the district court also found that "significant intervening events" between the discovery of the suspicious images on the Google servers and the discovery of the evidence in the defendant's apartment were sufficiently attenuated to purge the taint from any potentially unconstitutional search. *Id.*

The defendant pleaded guilty and reserved the right to appeal the denial of his motion. On appeal, the Fourth Circuit found that the Bedford County detective violated the Fourth Amendment by examining the three unopened images but agreed that the exclusionary rule did not apply on the facts of the case.

The government did not contest that the defendant had a subjective expectation of privacy in his Google cloud account, so the court declined to address that issue. Regarding whether the defendant's expectation of privacy in the account was objectively reasonable, the court rejected the notion that Google's privacy policy defeated any expectation of privacy. According to the court: "Every Google Drive user knows that Google may scan their files to see if those files contain anything illegal. But a user's knowledge that Google might occasionally sift through their files does not mean that he expects the Government to have unfettered access to those same files." *Id.* at 15. The court compared the situation to a person temporarily occupying a hotel room. While that person's privacy rights are somewhat diminished by the right of access of a hotel housekeeper to the room, the hotel guest is nonetheless protected against a warrantless search by police. "A Google Drive account is no different merely because it exists in the cyberworld." *Id.* at 16. The situation would be different where the government itself warns users of its computers that their internet use and files would be monitored. *See U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000) (so holding). The defendant here therefore retained a reasonable expectation of privacy in his cloud account.

He also had a reasonable expectation of privacy in the files uploaded to the Google account, notwithstanding their contraband nature. The district court erred by determining that the hash-matching algorithm was "exceedingly reliable," because no record evidence supported that proposition. It also erred by determining that the "hit" by the algorithm was akin to a canine alert in the automobile context. According to the court:

For one thing, Appellant's files were not in jeopardy of being lost or destroyed. Far from it. Google had copied each of the 156 files and sent them to NCMEC, which then forwarded them to law enforcement. Law enforcement easily could have obtained a warrant before opening the file, and any delay would not have hampered the investigations—the files were not going anywhere. . . They were instead hidden in a cloud based storage system, a digital filing cabinet of sorts, inaccessible to law enforcement. At the risk of stating the obvious, digital files are not automobiles. The two things are poles apart, and the Fourth Amendment treats them differently. *Lowers Slip op.* at 24-25.

As to the district court's private search reasoning, the court acknowledged a split of authority among the circuit courts about whether a hash-match can defeat a person's expectation of privacy in unopened digital files. The Ninth and Sixth Circuits have found that a hash-match does not overcome a person's privacy interest in digital files, while the Fifth and Sixth Circuits have found that it does. The Fourth Circuit agreed with the Ninth and Sixth Circuits. The hash-match itself did not reveal the contents of the files. Under the private search doctrine, a search by a private person—even an unreasonable one—does not violate the Fourth Amendment, and police may lawfully examine anything found by the private actor. However, police may not exceed the scope of the private search by conducting further warrantless searches. *U.S. v. Jacobsen*, 466 U.S. 109 (1984). Here, the Chesapeake detective exceeded the scope of the search by Google when she opened files that had not previously been examined by Google or NCMEC. "Because [the detective's] visual examination revealed information that the algorithm could not, the district court erred in concluding that her search did not exceed Google's private search. It clearly

did.” *Id.* at 33. Further, the fact that Google may have inspected a matching image uploaded by a different user at some earlier point in time could not frustrate the defendant’s expectation of privacy in the files he personally uploaded.

However, the district court correctly determined that suppression was inappropriate here, as the deterrent purpose of the exclusionary rule would not be served by excluding the evidence. Under *Utah v. Strieff*, 579 U.S. 232, 238 (2016), if “the causal connection between the unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance,” suppression is unwarranted. Courts use three factors to evaluate whether the discovery of evidence is sufficiently attenuated from the illegal search: 1) the passage of time between the search and the discovery of the evidence; 2) the existence of intervening circumstances; and 3) “the purpose and flagrancy of the official misconduct.” *Id.* Here, seven months passed between the illegal search and the later discovery of the evidence in the defendant’s apartment. The defendant voluntarily agreed to submit to two interviews with law enforcement (ultimately confessing in the second interview) and consented to searches of his digital devices. “Each of these intervening voluntary acts significantly attenuated the casual chain.” *Lowers Slip op.* at 43. Finally, the police misconduct at issue was “anything but flagrant.” *Id.* Application of the attenuation doctrine therefore precluded suppression, as any taint from the illegal search had dissipated by the time the evidence leading to prosecution was discovered. Given this decision, the court declined to address the reasoning of the district court regarding the good faith exception.

While the district court erred in finding no Fourth Amendment violation, it was correct as to the remedy, and its judgment was therefore affirmed.

Judge King wrote separately to concur. He would have joined the view of the Fifth and Sixth Circuits that any privacy interest the defendant had in the files was defeated by Google’s private search of the files.

Defendant with history of violent and unlawful conduct could be disarmed consistent with the Second Amendment; facial and as-applied challenges to firearm by felon rejected

[U.S. v. Holman](#), 171 F.4th 303 (March 27, 2026). After a night of drinking, the defendant crashed his car. This led to police to discover a stolen, loaded handgun and an extra ammunition magazine in his car. The defendant was a convicted felon, and the government charged him with possession of ammunition and possession of a firearm by a felon in the Middle District of North Carolina. He moved to dismiss, arguing facial and as-applied challenges to 18 U.S.C. 922(g)(1).

The Fourth Circuit rejected these arguments. In *U.S. v. Canada*, 123 F.4th 159, 161 (4th Cir. 2024), an earlier panel of the Fourth Circuit found that the statute “has a plainly legitimate sweep” and was facially constitutional. Under *U.S. v. Hunt*, 123 F.4th 697 (4th Cir. 2024), an earlier panel of the Fourth Circuit held that as-applied challenges to 922(g)(1) were limited to situations where the underlying conviction had been pardoned or where the underlying crime of conviction was found to be illegal or unconstitutional. The defendant did not fit into either exception, and the panel was bound by *Hunt* to reject his challenge. Assuming *arguendo* that *Hunt* did not apply to the defendant’s case, the panel nonetheless would have rejected it on the merits. His first felony conviction involved armed robbery; his second felony conviction involved possession of a firearm with a destroyed serial number. While serving his term of supervised release, the defendant had numerous violations, including using controlled substances, failing to complete substance abuse treatment, missing office visits with his probation officer, and more. The Second Amendment does not protect the gun rights of a person with the

defendant's history. Disarming such a person is also consistent with the Nation's historical tradition of firearm regulation insofar as there was a tradition of preventing "potentially violent or dangerous" people from possessing guns. *Holman* Slip op. at 7 (citation omitted). "Between *Canada*, *Hunt*, and the *Bruen* two-step, *Holman*'s Second Amendment challenge to his conviction fails multiple times over." *Id.*

Challenges to a sentencing enhancement for possession of a high-capacity magazine and to the reasonableness of his sentence were likewise rejected, and the judgment of the district court was unanimously affirmed in all respects.

Juror's comment to other jurors during deliberations that he knew the defendant's family and feared what would happen to them if the defendant was acquitted did not amount to improper external influence

[Daugherty v. Dingus](#), 171 F.4th 326 (March 30, 2026). The defendant was convicted in West Virginia state court of sexual abuse by a parent. During jury deliberations, one juror told the other jurors that he knew the defendant's family and was concerned about what would happen to the family if the defendant were acquitted. The defendant moved for a new trial in state court, arguing that this communication amounted to improper external influence on the jury deliberation process. The state post-conviction court denied relief, finding the juror's comments did not amount to improper external communication. That decision was affirmed by the West Virginia Supreme Court of Appeals ("WVSCA"). The defendant then renewed his arguments in federal habeas proceedings. The district court ultimately rejected his argument, finding that the WVSCA's decision did not unreasonably apply clearly established law. On appeal of that decision, the Fourth Circuit unanimously affirmed. In the words of the court:

Juror McBride's statements did not represent the kind of third-party communication clearly prohibited by [the U.S. Supreme Court]. There is no evidence of tampering by third parties outside the jury. The comments were not derived from any communication with other individuals during the trial and they did not originate from non-jury figures, such as law enforcement officers or bailiff. We agree with the State that McBride's comments 'came from his own mental machinations, whether true or not.' This is a far cry from the Supreme Court's limited precedent governing external influence. *Daugherty* Slip op. at 10.

Because the juror's comments—whether taken individually or collectively—did not amount to external influence on the deliberation process, the WVSCA's decision against the defendant was reasonable, and the defendant was not entitled to relief.